W. E. Burr
16 October1998
TWG-98-70

TWG Meeting Report 8 October 1998

The PKI TWG met on 8 October at the USPTO in Arlington Virginia.

Attendance

Bill Burr	NIST/Chair	Gene Hilborn	CSC
David Cooper	NIST	John Purcell	FSI-PMO
Nelson Hastings	NIST	Don Bronson	VA
David Moyer	Motorola	Jim Fisher	J. G. Van Dyke
Jack C. Sculer	Veterans Admin.	Kevin Hawkins	NTIS
Nick Haskakis	DISA	Matthew Hirsch	BAH
Lynn McNulty	RSA Data Security	Clem Boyleston	BMI
Claude Wilson	IBM	Carol Flaherty	EDS
Jerry Short	TRW	Chris Louden	NTIS
Frank Hecker	Netscape	Jack Ward	Infosec Services
Scott Lowry	DST	Roger Westman	IIT
Gregor Scott	DISA	MarcusBanjo	BAH
John Ward	INFOSEC Services	Eric Greenberg	DST/Seine Dynamics
Nicholas Harmon	PEC	Thomas Casey	PEC
Art Purcell	USPTO	Erik Pfeifer	PEC
MAJ Randall R. Vickers	IAESO DISA	Russ Davis	FDIC
LCDR Paul Friedrichs	DISA	Tom Crossan	State
N. Srinivaian		Bill Price	Mitre
RusselWeiser	Digital Signature Trust	Stephen Sill	DOT
Ed Anderson	Digital Signature Trust	Cecilia Williams	Control Data Systems
Cheryl Battan	Microsoft	Brian Leitner	BAH
Cathie Ward	Veterans Administration	Andrew Zimmerman	BAH
Artch Griffin	GSA/OGP	Thomas Brown	Communications Research and Consulting
Rich Bowler	DOJ/IMSS	Michael Umoleale	Control Data Systems
Bero Porter	GTE	Bill Curtin	DISA
Martin Smith	USITC	Laura Boyer	J. G. VanDyke
Phong Dang	USPTO	Orin Hamilton	USPTO
Rich Ankney	Certco	Patrick Arnold	Microsoft
Robert Campbell	Domain Tech	Willie Bolar	USPTO
Bill Bush	DoEd	Les Cashwell	Entrust
Pat Cain	BBN	Skip Chapman	Entrust
Steve Crawford	BAH	Andrew Csinger	GT Group Telecom.
Tice DeYoung	NASA	Donna Dodson	NIST
Kenneth W. Eggers	CygnaCom	Jan Lovorn	JL Information Sys.
Bernard Eydt	EDS	Salo Fajer	Domain Tecnologies
Dave Fillingham	NSA	Richard Guida	GITS/PKISC chair
Sharon Boeyen	Entrust	David Garver	Research @ Mgt. Sys.
Joanne Ghahremani	BTNA	Adam Safier	GEIS
Phillip Hallam-Baker	VeriSign	Jane Heinzman	JG VanDyke
Clay Holland	INS	Johnny Hsiung	Cygnacom
Kathleen Koziana	Compaq	Dick Lasocki	

Abby MacLean	RAMS, Inc.	Julie Smith McEwen	T. Rowe Price
Sandi Miklos	NSA	L. E. Morton	AT&T
Noel Nazario	NIST	Jennifer Nowell	J. G. VanDyke
Mike Pfeferstein	FHFB	Steve Peterson	Chromatix
Keith Gorlen	NIH	Tim Polk	NIST
Ted Slusarczyk	Commerce	Marian A. Royal	GSA E-mail PMO
Bob Patterson	USPTO	David Simonetti	BAH
Robert Malick	NIH	Barbara Staples	Mitretek
Graeme Thomson	Data Connection Ltd.	D. G. Sweigert	J. G. Van Dyke
Sandy Orlow	NIH	George Usher	CORBETT Tech.
Drew M Powles	TASC	All Williams	Security Bus. Sol.
Kathy Lyons-Burke	NIST	Jim Bates	BAH
Dan Wu	DISA	Tom Llanso	Chromatix
J. Sandhu	LockheedMartin	Mickey Tevelow	Dept. of Energy
Jerry Oar	SphereCom Enterprises	Tina R. Fox	US Customs
Pedro Haworth	Litton/PRC	Tim Hurr	AT&T
Don Brewer	boeing IS	Lloyd Smith	SSA
Pete Hogan	Telos Corp	Rik Andrews	Netscape

Discussion

The meeting focused on Directory Issues

- Sharon Boeyen (Entrust) made a presentation: Directory Technologies for PKI Repositories <http://csrc.nist.gov/pki/twg/presentations/twg-98-67.pdf>. Sharon's presentation was an overview of standards based directory technologies (X.500 & LDAP) applicable to a PKI. she identified a number of the issues involved in setting up a directory for use with a PKI. Sharon stated that X.500 does satisfy all PKI repository requirements, however LDAP is more widely implemented and therefore is the repository access protocol of choice. Many X.500 compliant directories offer LDAP front ends and the combination of LDAP access to X.500 based directories does the best job of any existing technology of serving PKI needs.
- Frank Hecker (Netscape) made a presentation: Basics of Lightweight Directory Access Protocol <http://csrc.nist.gov/pki/twg/presentations/twg-98-69.pdf>. Frank described the history of LDAP and the reasons for its creation. The LDAP data model is based on X.500, and has a standard set of attribute syntaxes corresponding to the X.500 schema. Therefore the two are not incompatible, however LDAP V2 tends to return data in "printable string" form and this is a limitation for languages that use other character sets. LDAP V2 paid little attention to access control and security. LDAP V3 (now just coming into use) supports additional operations, the use of the UTF-8 character set, "binary blobs" (useful for signed objects), and improved security, however there is still no standard for access control. A great deal of work is in progress to further extend LDAP (including access control). Frank pointed out that the application of LDAP directories is not simply "phone book" or PKI applications but also as a part of the fabric of distributed systems to hold configuration information, user preferences and the like. This helps to facilitate both management and user mobility in distributed systems. Development of LDAP ins now in the IETF and PKIX references LDAP V2. For PKI there is a certificate format issue with LDAP V2, which is handled in V3 by the "binary blobs."
- Marion Royal (GSA) made a presentation: "Overview of the Directory Forum Federal White Pages Initiative and U.S. Government On-Line Directories (USGold)" <http://csrc.nist.gov/pki/twg/presentations/twg-98-68.pdf>. Marion described the current unorganized condition of numerous government directories, which are locally useful, but generally not globally accessible. The US Gold Pilot was a trial of a Government-wide directory, based on X.500. As a next

step in this effort the Directory Forum has been established with the goal in the next step to make accessible (inside and outside the Government) listings for 80% of government employees by 3rd quarter of FY 99. The US Gold directory will tie together existing diverse technologies, including X.500, LDAP directories, databases, proprietary e-mail directories and web page personnel locators. The kickoff meeting of the Directory Forum was held sept.29, and the next meetings will be Oct. 27 and Dec 8. Send a message to listproc@ds2.fed.gov with "subscribe dirmaster-L <your name>" in the body of the message to be added to the Directory Forum discussion list.

- Sandy Miklos (NSA) made a presentation: "Certificate Repository Security Discussions" <http://csrc.nist.gov/pki/twg/presentations/twg-98-63.pdf> Sandy discussed the security issues in a large directory system and directory issues in general. Threats include: replay, manipulation, masquerade, data modification, and denial of service. The repository publish and provide access to: user public key certificates, CA public key certificates, CA cross certificates, CRLs, ARLs, and other related attributes such as policies. Sandy discussed role separation, audit information, authentication of operators and users, and access control. Sandy concluded that no access control should be required to read attributes (at least for most civil agencies), but strong access control is required for operators/administrators and for CAs to update PKI information in directories. 7 x 24 availability is key for directories. The X.500 standard presently provides the best options for access control; although LDAP V3 improves the LDAP picture, it is not clear how well LDAP will implement the full security features of X.500, including permissions, precedence and access control. A threat assessment and an organizational security policy are needed, and as well as assurance requirements for the Federal PKI as a whole and the individual elements of the FPKI
- Laura Boyer (J. G. Van Dyke) made a presentation "Implementation Directories " <http://csrc.nist.gov/pki/twg/presentations/twg-98-65.pdf>. It was based on her experience implementing directories for different clients. The directory is the key component for information management, not simply an adjunct to a PKI. Laura provided a long list of directory design issues, beginning with identifying the authoritative sources for data. She unidentified a number of interoperability issues including the protocol versions supported, and ASN.1 encoding inconsistencies (encoding must be preserved for signatures to work). Although support for shadowing is an explicit feature of the 1993 X.500 standard, it has proved to be problematic, with little inter-vendor interoperability. She also provided a long list of directory security issues.
- Steve Peterson (Chromatix) presented: "Directory Security Brief", which was based on the experience of Chromatix as a directory vendor. <http://csrc.nist.gov/pki/twg/presentations/twg-98-66.pdf> Chromatix is a vendor of secure X.500 and LDAP directory products and security and directory services. Two contrasting approaches are signed X.518 directory access operations versus SSL/TLS directory access. While certificates and CRLs are self-authenticating, directories may contain critical data (e.g. configuration or routing data) that is not signed and must be protected. Denial of service attacks are a threat. X.500 and LDAP error messages make it difficult to isolate precise errors. Decoding (for storage in the directory) and re-encoding problems interfere with the preservation of signed objects, and there are particular incompatibilities between the 1988 and 1993 versions of x.500. Clock synchronization is a problem for X.518 and X.511.
- LCDR Paul Friedrichs (DISA) presented: "DoD Medium Assurance PKI Major Directory Challenges" <http://csrc.nist.gov/pki/twg/presentations/twg-98-64.pdf>. Commander Friedrichs discussed some of the problems the he is encountering as chief engineer for the DoD Medium Assurance PKI effort, which is standards based and uses COTS products. A first, and rather surprising problem, is that COTS directory clients do not support multiple certificates for the same user, although the directories can contain them. DoD is using separate signature and encryption certificates (needed for key recovery) and is having to stand up two separate directory structures to make both accessible to the clients. More profoundly, Commander Freidrichs doesn't think that the single directory information tree view of data, with management by subtrees, meets the needs of a large, diverse organization like DoD. He feels that the performance needs of DoD could best be met by a large scale centralized directory server,

but that the COTS products don’t begin to address the management of such a directory or the issues involved in delegating the control of the many attributes that should be contained in such a directory.

The presentations were followed by a discussion. Bill Burr posed the question, why do we need an LDAP protocol that seems to be growing to duplicate all the features of X.500, what is lightweight about it when that happens? A plausible answer: X.500, conceived as a complete solution was too vast to meet the product needs of vendors; X.500 implementations have necessarily been subsets, and almost always different subsets, hence many of the interoperability problems of different products. LDAP is being done in more digestible chunks; while the solutions are not as complete as conceived by X.500 and DAP, they are easier to reduce to products, and do meet specific needs well. The attempts of standards committees to design comprehensive solutions for the ages have rarely prevailed over more incremental and pragmatic approaches. Phillip Hallam-Baker stressed that directory and PKI technologies are both rapidly evolving and asserted that it would be a mistake to try to hitch PKI to tightly to a particular directory approach, while this evolution is progressing so rapidly.

There was general agreement that some flavor of LDAP (V2 or V3 is less clear) is, for better or worse, going to be the industry standard. The back end of directories and issues such as shadowing, chaining, and referrals more uncertain and we may have accommodate considerable heterogeneity. Often it is the very limited client capabilities that are the most constraining aspect of present COTS products. Noel Nazario volunteered to take the lead in generating a “wish list” for directories and clients.

Action Items:
- Cashwell: briefing on IKE
- Nazario: Draft of Directory features list.
- Burr: contact NACHA concerning a briefing on their pilot;

The next TWG meeting will be 12 Nov. at BAH, Airport Square #2 near BWI airport.